
ISO 27001:2022

**Seguridad de la información,
ciberseguridad y protección de la
privacidad.**

**Sistemas de gestión de la seguridad de la
información**

ADVERTENCIA

**Esta norma no forma parte
del material del curso. Es sólo
para uso interno de TÜV
Rheinland Group.**

**Por favor, destruya la misma
al finalizar el curso**

Índice

Prólogo	5
0 Introducción.....	6
0.1 Generalidades.....	6
0.2 Compatibilidad con otras normas de sistemas de gestión	6
1 Objeto y campo de aplicación.....	7
2 Normas para consulta.....	7
3 Términos y definiciones.....	7
4 Contexto de la organización	7
4.1 Comprensión de la organización y de su contexto	7
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	7
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información.....	8
4.4 Sistema de gestión de la seguridad de la información.....	8
5 Liderazgo	8
5.1 Liderazgo y compromiso.....	8
5.2 Política.....	9
5.3 Roles, responsabilidades y autoridades en la organización.....	9
6 Planificación.....	10
6.1 Acciones para tratar los riesgos y oportunidades.....	10
6.1.1 Consideraciones generales	10
6.1.2 Evaluación de los riesgos de seguridad de la información.....	10
6.1.3 Tratamiento de los riesgos de seguridad de la información	11
6.2 Objetivos de seguridad de la información y planificación para su consecución	12
6.3 Planificación de cambios	13
7 Soporte	13
7.1 Recursos.....	13
7.2 Competencia.....	13
7.3 Concienciación.....	13
7.4 Comunicación	13
7.5 Información documentada.....	14
7.5.1 Consideraciones generales	14
7.5.2 Creación y actualización	14
7.5.3 Control de la información documentada	14
8 Operación	15
8.1 Planificación y control operacional	15
8.2 Evaluación de los riesgos de seguridad de la información.....	15
8.3 Tratamiento de los riesgos de seguridad de la información	15
9 Evaluación del desempeño.....	16
9.1 Seguimiento, medición, análisis y evaluación.....	16

9.2	Auditoría interna.....	16
9.2.1	Consideraciones generales	16
9.2.2	Programa de auditoría interna	16
9.3	Revisión por la dirección.....	17
9.3.1	Consideraciones generales	17
9.3.2	Entradas de la revisión por la dirección	17
9.3.3	Resultados de la revisión por la Dirección.....	18
10	Mejora.....	18
10.1	Mejora continua	18
10.2	No conformidad y acciones correctivas.....	18
Anexo A (Normativo)	Controles de la seguridad de la información de referencia	19
Bibliografía.....		29

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase www.iso.org/directives).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de alguno o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de este documento se indicarán en la Introducción y/o en la lista ISO de declaraciones de patente recibidas (véase www.iso.org/patents).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html.

Este documento ha sido elaborado por el Comité Técnico ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Seguridad de la información, ciberseguridad y protección de la privacidad*.

Esta tercera edición anula y sustituye a la segunda edición (ISO 27001:2013) que ha sido revisada técnicamente. También incorpora el Corrigendum Técnico ISO/IEC 27001:2013/Cor 1:2014 y ISO/IEC 27001:2013/Cor 2:2015.

Los cambios principales en comparación con la edición previa son los siguientes:

- el texto se ha alineado con la estructura armonizada de normas de sistemas de gestión e ISO/IEC 27002:2022.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En www.iso.org/members.html se puede encontrar un listado completo de estos organismos.

0 Introducción

0.1 Generalidades

Este documento se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información por una organización está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Es previsible que todos estos factores condicionantes cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.

Es importante que el sistema de gestión de la seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la implementación del sistema de gestión de la seguridad de la información se ajuste a las necesidades de la organización.

Este documento puede ser utilizado por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad.

El orden en que este documento presenta los requisitos no es reflejo de su importancia ni implica el orden en el cual deben implementarse. Los elementos de cada listado se enumeran sólo a título de referencia.

La Norma ISO/IEC 27000 describe la visión de conjunto y el vocabulario de los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de la seguridad de la información (incluyendo las Normas ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4]), junto con los términos y definiciones relacionados.

0.2 Compatibilidad con otras normas de sistemas de gestión

Este documento emplea la estructura de alto nivel, texto esencial idéntico, términos y definiciones esenciales comunes contenidos en el anexo SL de la Parte 1 de las Directivas ISO/IEC, Suplemento ISO consolidado y por lo tanto mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el anexo SL.

Este enfoque común definido en el anexo SL será útil para aquellas organizaciones que deciden implantar un sistema de gestión que cumpla con los requisitos de dos o más normas de sistemas de gestión.

1 Objeto y campo de aplicación

Este documento especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización. Este documento también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en este documento son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza. No se acepta la exclusión de cualquiera de los requisitos especificados en los capítulos 4 al 10 cuando la organización reclame la conformidad con este documento.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluida cualquier modificación de esta).

ISO/IEC 27000, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.*

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma ISO/IEC 27000.

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

- Plataforma de búsqueda en línea de ISO: disponible en <http://www.iso.org/obp>
- Electropedia de IEC: disponible en <http://www.electropedia.org/>

4 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado 5.4.1 de la Norma ISO 31000:2018[5].

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

- a) las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información;

- b) los requisitos relevantes de estas partes interesadas;
- c) cuales de estos requisitos se abordarán a través del sistema de gestión de la seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, así como obligaciones contractuales.

4.3 Determinación del alcance del sistema de gestión de la seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

- a) las cuestiones externas e internas referidas en el apartado 4.1;
- b) los requisitos referidos en el apartado 4.2;
- c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de la seguridad de la información

La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, incluyendo los procesos requeridos y sus interacciones de acuerdo con los requisitos de este documento.

5 Liderazgo

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

- a) asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;
- b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;
- c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;
- d) comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información;

- e) asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos;
- f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;
- g) promoviendo la mejora continua; y
- h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

NOTA La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

- a) sea adecuada al propósito de la organización;
- b) incluya objetivos de seguridad de la información (véase 6.2) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información;
- c) incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e
- d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información debe:

- e) estar disponible como información documentada;
- f) comunicarse dentro de la organización;
- g) estar disponible para las partes interesadas, según sea apropiado.

5.3 Roles, responsabilidades y autoridades en la organización

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de este documento;
- b) informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el comportamiento del sistema de gestión de la seguridad de la información dentro de la organización.

6 Planificación

6.1 Acciones para tratar los riesgos y oportunidades

6.1.1 Consideraciones generales

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:

- a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;
- b) prevenir o reducir efectos indeseados;
- c) lograr la mejora continua.

La organización debe planificar:

- d) las acciones para tratar estos riesgos y oportunidades; y
- e) la manera de:
 - 1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y
 - 2) evaluar la eficacia de estas acciones.

6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de los riesgos de seguridad de la información que:

- a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
 - 1) los criterios de aceptación de los riesgos, y
 - 2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;
- b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;
- c) identifique los riesgos de seguridad de la información:
 - 1) llevando a cabo el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,
 - 2) identificando a los dueños de los riesgos;

d) analice los riesgos de seguridad de la información:

- 1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,
- 2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),
- 3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

- 1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),
- 2) priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

6.1.3 Tratamiento de los riesgos de seguridad de la información

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

- a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;
- b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA 1 Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

- c) comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

NOTA 2 El anexo A contiene una lista de posibles controles de seguridad de la información. Se indica a los usuarios de este documento que se dirijan al anexo A para asegurar que no se pasan por alto controles necesarios.

NOTA 3 Los controles de seguridad de la información enumerados en el anexo A no son exhaustivos, por lo que pueden ser necesarios controles de seguridad de la información adicionales.

d) elaborar una “Declaración de Aplicabilidad” que contenga:

- los controles necesarios [véase 6.1.3 b) y c)];
- la justificación de las inclusiones;
- si los controles necesarios están implementados o no; y
- la justificación de las exclusiones de cualquiera de los controles del anexo A;

- e) formular un plan de tratamiento de riesgos de seguridad de la información; y
- f) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA 4 La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en este documento se alinean con los principios y directrices genéricas definidos en la Norma ISO 31000[5].

6.2 Objetivos de seguridad de la información y planificación para su consecución

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

- a) ser coherentes con la política de seguridad de la información;
- b) ser medibles (si es posible);
- c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos;
- d) ser monitorizados;
- e) ser comunicados;
- f) ser actualizados, según sea apropiado;
- g) estar disponibles como información documentada.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:

- h) lo que se va a hacer;
- i) qué recursos se requerirán;
- j) quién será responsable;
- k) cuándo se finalizará; y
- l) cómo se evaluarán los resultados.

6.3 Planificación de cambios

Cuando la organización determine la necesidad de cambios en el sistema de gestión de la seguridad de la información, estos cambios se deben llevar a cabo de manera planificada.

7 Soporte

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

7.2 Competencia

La organización debe:

- a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y
- b) asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;
- c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y
- d) conservar la información documentada apropiada, como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3 Concienciación

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

- a) la política de la seguridad de la información;
- b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información;
- c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

- a) el contenido de la comunicación;

- b) cuándo comunicar;
- c) con quién comunicar;
- d) cómo comunicar.

7.5 Información documentada

7.5.1 Consideraciones generales

El sistema de gestión de la seguridad de la información de la organización debe incluir:

- a) la información documentada requerida por este documento;
- b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

- 1) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,
- 2) la complejidad de los procesos y sus interacciones, y
- 3) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

- a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
- b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);
- c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por este documento se debe controlar para asegurarse que:

- a) esté disponible y preparada para su uso, dónde y cuándo se necesite;
- b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

- c) distribución, acceso, recuperación y uso;

- d) almacenamiento y preservación, incluida la preservación de la legibilidad;
- e) control de cambios (por ejemplo, control de versión);
- f) conservación y disposición.

La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de la calidad, se debe identificar, según sea apropiado, y controlar.

NOTA El acceso puede implicar una decisión en relación con el permiso, solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos, y para implementar las acciones determinadas en el capítulo 6:

- estableciendo criterios para los procesos;
- implementando controles en los procesos de acuerdo con los criterios.

En la medida necesaria la organización debe tener disponible información documentada, para tener la confianza de que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario.

La organización debe garantizar que los procesos, productos o servicios proporcionados externamente y relevantes para el sistema de gestión de la seguridad de la información estén controlados.

8.2 Evaluación de los riesgos de seguridad de la información

La organización debe efectuar evaluaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a).

La organización debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

8.3 Tratamiento de los riesgos de seguridad de la información

La organización debe implementar el plan de tratamiento de los riesgos de seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- a) a qué es necesario monitorizar y medir, incluyendo procesos y controles de seguridad de la información;
- b) los métodos de monitorización, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos;
- c) cuándo se deben llevar a cabo el seguimiento y la medición;
- d) quién debe hacer el seguimiento y la medición;
- e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;
- f) quién debe analizar y evaluar esos resultados.

La organización debe tener disponible la información documentada apropiada como evidencia de los resultados.

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

9.2 Auditoría interna

9.2.1 Consideraciones generales

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

- a) cumple con:
 - 1) los requisitos propios de la organización para su sistema de gestión de la seguridad de la información,
 - 2) los requisitos de este documento,
- b) está implementado y mantenido de manera eficaz.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes.

Al establecer el programa o programas de auditoría interna, la organización debe tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas.

La organización debe:

- a) para cada auditoría, definir sus criterios y su alcance;
- b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; y
- c) asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías.

Se debe tener disponible información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.

9.3 Revisión por la dirección

9.3.1 Consideraciones generales

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir consideraciones sobre:

- a) el estado de las acciones de anteriores revisiones por la dirección;
- b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;
- c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de la seguridad de la información;
- d) la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a:
 - 1) no conformidades y acciones correctivas,
 - 2) seguimiento y resultados de las mediciones,
 - 3) resultados de auditoría,
 - 4) el cumplimiento de los objetivos de seguridad de la información;
- e) los comentarios provenientes de las partes interesadas;
- f) los resultados de la evaluación de los riesgos y el estado del plan de tratamiento de riesgos;
- g) las oportunidades de mejora continua.

9.3.3 Resultados de la revisión por la Dirección

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización debe tener disponible información documentada como evidencia de los resultados de las revisiones por la dirección.

10 Mejora

10.1 Mejora continua

La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

10.2 No conformidad y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

- a) reaccionar ante la no conformidad, y según sea aplicable:
 - 1) llevar a cabo acciones para controlarla y corregirla,
 - 2) hacer frente a las consecuencias;
- b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante:
 - 1) la revisión de la no conformidad,
 - 2) la determinación de las causas de la no conformidad, y
 - 3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;
- c) implementar cualquier acción necesaria;
- d) revisar la eficacia de las acciones correctivas llevadas a cabo; y
- e) si es necesario, hacer cambios al sistema de gestión de la seguridad de la información.

Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas.

La organización debe tener disponible información documentada, como evidencia de:

- f) la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo;
- g) los resultados de cualquier acción correctiva.

Anexo A (Normativo)

Controles de la seguridad de la información de referencia

Los controles de seguridad de la información que se enumeran en la tabla A.1 se corresponden directamente con los que figuran en la Norma ISO/IEC 27002:2022[1], capítulos 5 a 8, y deben ser empleados en el contexto del apartado 6.1.3.

Tabla A.1 – Controles de la seguridad de la información

5	Controles organizacionales	
5.1	Políticas para la seguridad de la información	<p>Control</p> <p>La política de seguridad de la información y un conjunto de políticas temáticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.</p>
5.2	Roles y responsabilidades en seguridad de la información	<p>Control</p> <p>Todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.</p>
5.3	Segregación de tareas	<p>Control</p> <p>Las funciones y áreas de responsabilidad en conflicto deben segregarse.</p>
5.4	Responsabilidades de la dirección	<p>Control</p> <p>La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información, las políticas temáticas y sus procedimientos específicos establecidos en la organización.</p>
5.5	Contacto con las autoridades	<p>Control</p> <p>Deben establecerse y mantenerse los contactos adecuados con las autoridades pertinentes.</p>
5.6	Contacto con grupos de interés especial	<p>Control</p> <p>Deben establecerse y mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.</p>
5.7	Inteligencia de amenazas	<p>Control</p> <p>La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas.</p>

5.8	Seguridad de la información en la gestión de proyectos	Control La seguridad de la información debe integrarse en la gestión de proyectos.
5.9	Inventario de información y otros activos asociados	Control Debe elaborarse y mantenerse un inventario de la información y otros activos asociados, incluyendo la identificación de sus propietarios.
5.10	Uso aceptable de la información y activos asociados	Control Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de información y otros activos asociados.
5.11	Devolución de activos	Control Todos los empleados y otras terceras partes, según procedan, deben devolver todos los activos de la organización en su poder tras el cambio o la terminación de su trabajo, contrato o acuerdo.
5.12	Clasificación de la información	Control La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	Etiquetado de la información	Control Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
5.14	Transferencia de la información	Control Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de medios de transferencia dentro de la organización y entre la organización y otras partes.
5.15	Control de acceso	Control Se deben establecer e implementar reglas de control de acceso físico y lógico a la información y otros activos asociados, basadas en los requisitos de negocio y de seguridad de la información.
5.16	Gestión de identidad	Control Se debe gestionar el ciclo de vida completo de las identidades.
5.17	Información de autenticación	Control La asignación y gestión de la información de autenticación debe controlarse mediante un proceso formal de gestión, incluyendo el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación.

5.18	Derechos de acceso	<p>Control</p> <p>Los derechos de acceso a la información y otros activos asociados deben aprovisionarse, revisarse, modificarse y eliminarse de conformidad con la política específica de la organización y las reglas sobre control de acceso.</p>
5.19	Seguridad de la información en las relaciones con los proveedores	<p>Control</p> <p>Se deben identificar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores.</p>
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	<p>Control</p> <p>Deben establecerse y acordarse con cada proveedor los requisitos pertinentes de seguridad de la información en función del tipo de relación con el proveedor.</p>
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	<p>Control</p> <p>Se deben definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de Tecnologías de la Información y de las Comunicaciones (TIC).</p>
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	<p>Control</p> <p>La organización debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información y prestación de servicios de los proveedores.</p>
5.23	Seguridad de la información para el uso de servicios en la nube	<p>Control</p> <p>Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.</p>
5.24	Planificación y preparación de la gestión de incidentes de seguridad de información	<p>Control</p> <p>La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, roles y responsabilidades de gestión de los incidentes de seguridad de la información.</p>
5.25	Evaluación y decisión sobre los eventos de seguridad de información	<p>Control</p> <p>La organización debe evaluar los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información.</p>
5.26	Respuesta a incidentes de seguridad de la información	<p>Control</p> <p>Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.</p>

5.27	Aprender de los incidentes de seguridad de la información	Control El conocimiento adquirido a partir de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.
5.28	Recopilación de evidencias	Control La organización debe establecer e implementar procedimientos para la identificación, recogida, adquisición y preservación de evidencias relacionadas con eventos de seguridad de la información.
5.29	Seguridad de la información durante la interrupción	Control La organización debe planificar cómo mantener la seguridad de la información a un nivel adecuado durante la Interrupción.
5.30	Preparación para las TIC para la continuidad del negocio	Control La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
5.31	Identificación de requisitos legales, reglamentarios y contractuales	Control Los requisitos legales, estatuarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenerse actualizados.
5.32	Derechos de propiedad intelectual (DPI)	Control La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual (DPI).
5.33	Protección de los registros	Control Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
5.34	Privacidad y protección de datos de carácter personal (DCP)	Control La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
5.35	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidos los procesos, la tecnología y las personas, debe revisarse de forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.

5.36	Cumplimiento de las políticas y normas de seguridad de la información	Control Debe comprobarse periódicamente el cumplimiento con la política de seguridad de la información, las políticas temáticas específicas, las reglas y las normas de la organización.
5.37	Documentación de procedimientos operacionales	Control Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.
6	Personas	
6.1	Comprobación	Control La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo antes de unirse a la organización y de forma continua, de acuerdo con las leyes, reglamentos y éticas aplicables, y debe ser proporcional a los requisitos empresariales, la clasificación de la información a la que se accederá y los riesgos percibidos.
6.2	Términos y condiciones de contratación	Control Los acuerdos contractuales de empleo deben indicar las responsabilidades del personal y de la organización en materia de seguridad de la información.
6.3	Concienciación, educación y formación en seguridad de la información	Control El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concienciación, educación y formación sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.
6.4	Proceso disciplinario	Control Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
6.5	Responsabilidad ante la finalización o cambio	Control Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cese o cambio de empleo se deben definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.
6.6	Acuerdos de confidencialidad o no divulgación	Control Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.

6.7	Teletrabajo	Control Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
6.8	Notificación de los eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal notifique a tiempo eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.
7	Infraestructura	
7.1	Perímetro de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger áreas que contengan información y otros activos asociados.
7.2	Controles físicos de entrada	Control Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.
7.3	Seguridad de oficinas, despachos y recursos	Control Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
7.4	Monitorización de la seguridad física	Control Las instalaciones deben ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.
7.5	Protección contra las amenazas físicas y ambientales	Control Se debe diseñar e implementar una protección a las infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.
7.6	El trabajo en áreas seguras	Control Se debe diseñar e implementar procedimientos para trabajar en las áreas seguras.
7.7	Puesto de trabajo despejado y pantalla limpia	Control Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.
7.8	Emplazamiento y protección de equipos	Control Los equipos deben situarse de forma protegida y segura.
7.9	Seguridad de los equipos fuera de las instalaciones	Control Los activos fuera de las instalaciones deben estar protegidos.

7.10	Soportes de almacenamiento	Control Los soportes de almacenamiento deben gestionarse durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	Instalaciones de suministro	Control Las instalaciones de procesamiento de información deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
7.12	Seguridad del cableado	Control El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
7.13	Mantenimiento de los equipos	Control Los equipos deben recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación o reutilización segura de equipos	Control Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia, han sido eliminados o sobrescritos de manera segura, antes de deshacerse de ellos o reutilizarlos.
8	Tecnología	
8.1	Dispositivos finales de usuario	Control La información almacenada, procesada o accesible a través de dispositivos finales de usuario debe protegerse.
8.2	Gestión de privilegios de acceso	Control La asignación y el uso de derechos de acceso con privilegios deben restringirse y controlarse.
8.3	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y otros activos relacionados, de acuerdo con las políticas específicas de control de acceso definidas.
8.4	Acceso al código fuente	Control Se debe gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.
8.5	Autenticación segura	Control Las tecnologías y procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.

8.6	Gestión de capacidades	<p>Control</p> <p>Se debe supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.</p>
8.7	Controles contra el código malicioso	<p>Control</p> <p>Se debe implementar una protección contra el código malicioso, respaldada por una concienciación adecuada al usuario.</p>
8.8	Gestión de vulnerabilidades técnicas	<p>Control</p> <p>Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas.</p>
8.9	Gestión de la configuración	<p>Control</p> <p>Se debe ser establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.</p>
8.10	Eliminación de la información	<p>Control</p> <p>La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.</p>
8.11	Enmascaramiento de datos	<p>Control</p> <p>El enmascaramiento de datos debe utilizarse de acuerdo con la política específica del tema de la organización sobre el control de acceso, con otras políticas temáticas relacionadas, así como con los requisitos de negocio, teniendo en cuenta los requisitos legales aplicables.</p>
8.12	Prevención de fugas de datos	<p>Control</p> <p>Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.</p>
8.13	Copias de seguridad de la información	<p>Control</p> <p>Las copias de seguridad de la información, del software y de los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad específica acordada.</p>
8.14	Redundancia recursos de tratamiento de la información	<p>Control</p> <p>Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.</p>
8.15	Registros de eventos	<p>Control</p> <p>Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.</p>

8.16	Seguimiento de actividades	<p>Control</p> <p>Las redes, los sistemas y las aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.</p>
8.17	Sincronización del reloj	<p>Control</p> <p>Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.</p>
8.18	Uso de los programas de utilidad con privilegios	<p>Control</p> <p>Se debe restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.</p>
8.19	Instalación del software en sistemas en producción	<p>Control</p> <p>Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas en producción.</p>
8.20	Seguridad de redes	<p>Control</p> <p>Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.</p>
8.21	Seguridad de los servicios de red	<p>Control</p> <p>Se deben identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.</p>
8.22	Segregación en redes	<p>Control</p> <p>Los grupos de servicios de información, de usuarios y de sistemas de información deben ser segregados en las redes de la organización.</p>
8.23	Filtrado de webs	<p>Control</p> <p>El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.</p>
8.24	Uso de la criptografía	<p>Control</p> <p>Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida para la gestión de claves criptográficas.</p>
8.25	Seguridad en el ciclo de vida del desarrollo	<p>Control</p> <p>Se deben establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas.</p>

8.26	Requisitos de seguridad de las aplicaciones	Control Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
8.27	Arquitectura segura de sistemas y principios de ingeniería	Control Los principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.
8.28	Codificación segura	Control Principios de codificación segura deben aplicarse al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación	Control Deben definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.
8.30	Externalización del desarrollo	Control La organización debe controlar, monitorizar y revisar las actividades relativas al desarrollo externalizado de sistemas.
8.31	Separación de los entornos de desarrollo, prueba y producción	Control Deben separarse y protegerse los entornos de desarrollo, prueba y producción.
8.32	Gestión de cambios	Control Los cambios en las instalaciones de tratamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	Datos de prueba	Control Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Control Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.

Bibliografía

- [1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection. Information security controls.*
- [2] ISO/IEC 27003, *Information technology. Security techniques. Information security management systems. Guidance.*
- [3] ISO/IEC 27004, *Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.*
- [4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection. Guidance on managing information security risks.*
- [5] ISO 31000:2018, *Risk management. Guidelines.*